THE CLAIMS

A complete listing of all of originally filed Claims 1 - 33 is provided below. A status identifier is provided for each claim in a parenthetical expression following each claim number.

1. (Previously Presented) A distributed firewall (DFW) for use on an end system, comprising:

an end system authentication component for providing user authentication for connection attempts from users attempting to access the end system via a network;

an end system access control component for providing purpose authorization for authenticated users based on rules in a connection policy associating users with purposes; and

an end system enforcement component for enforcing the connection policy rule for one of the authenticated users from whom traffic is received at the end system; ~~and~~

wherein the end system authentication component utilizes an aggregate of the users in the connection policy to authenticate at least one of the users.

2. (Currently Amended) The DFW of claim 1, wherein the end system authentication component utilizes Internet key exchange (IKE) protocol to authenticate users in IKE main mode (MM) based on the aggregate of users in the connection policy.

3. (Currently Amended) The DFW of claim 2, wherein the end system authentication component utilizes the rule in the connection policy associated with the authenticated user in IKE quick mode (QM) to complete the authentication.

4. (Currently Amended) The DFW of claim 3, wherein the end system authentication component transmits a secure notify message to the authenticated user when the authenticated user sends traffic in QM that exceeds an authority governed by the rule in the connection policy associated with the authenticated user.

5. (Currently Amended) The DFW of claim 3, wherein the end system enforcement component utilizes Internet protocol security (IPSec) protocol to maintain security of communications from the authenticated user when the communications are within the rule in the connection policy.

6. (Currently Amended) The DFW of claim 5, wherein the end system enforcement component enables IPSec on a socket for communications from the authenticated user and binds the socket in exclusive mode so that the context of the binder of the socket is preserved.

7. (Currently Amended) The DFW of claim 1, further comprising an end system inspection component for inspecting packets from an authenticated user.

8. (Original) The DFW of claim 1, wherein the connection policy is defined in a pluggable policy component.

9. (Original) The DFW of claim 8, wherein the pluggable policy component is downloaded from a centralized administrative policy.

10. (Original) The DFW of claim 8, wherein the pluggable policy component is modifiable on the end system.

11. (Currently Amended) The DFW of claim 10, further comprising an end system access control component through which the connection policy may be defined.

12. (Currently Amended) The DFW of claim 1, further comprising an end system access control component having a user interface (UI) through which the connection policy is defined.

13 - 33. (Withdrawn)